CPNI

Policies & Procedures Manual

February 23, 2009

Introduction

Under FCC regulations, all telecommunications carriers are required to protect the privacy of their customers. The "I3 BROADBAND CPNI Policies & Procedures" manual has been put into place in order to ensure I3 BROADBAND follows the FCC privacy guidelines. A copy of the complete CPNI Compliance Manual, issued by the FCC, has been electronically issued to every employee and is posted in every department of the I3 BROADBAND office.

Customer Proprietary Network Information, or CPNI, is certain customer information obtained by a telecommunications provider during the course of providing service to a customer. This includes information relating to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier. CPNI may also include information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

According to the FCC, CPNI encompasses "where, when and to whom" a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent to which the service is used.

CPNI also includes information typically contained in Call Detail Records, such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls. It also includes the additional services and features purchased by the consumer, such as call waiting, Caller ID, etc. CPNI, therefore, contains not only private, personal information, but commercially-sensitive information, as well.

CPNI does not include a customer's name, phone number and address aggregate customer information. Also not included under the definition is "subscriber list information" when included in a telephone directory or publicly available through other means. However, the names, addresses, and telephone numbers of UNLISTED customers are not subscriber list information.

Failure to comply with the guidelines listed in the I3 BROADBAND CPNI Policies & Procedures and the CPNI Compliance Manual will result in the following disciplinary actions:

1st offense – written warning will be issued
2nd offense – employee termination

Customer Interaction

Customer CPNI Protection Methods

1. CPNI information cannot be visible or accessible when unattended.
2. Customers can not be allowed into an office area where other customer's CPNI information is visible either on a desktop or on a computer.
3. When service is established, an account password is required to activate a customer account.

Customer Authentication Methods

1. CPNI information cannot be provided, via the telephone, without providing the customer's pre-established account password.
2. CPNI information can be provided by mail to the address of record or to the phone number of record.
3. Access to CPNI information can be provided if a valid photo ID is presented by either the account owner or a contact listed on the account.

Customer Notification of CPNI Changes

1. Customers will be automatically emailed a notification when the following items are changed on their account:
    a. Password modification
    b. Address of record change or creation
    c. Online password or auto pay changes
    d. Online payment is made on account
    e. Password Retrieval for Customers through the I3 BROADBAND website

Sales

Sales and Marketing Campaign Approval

1. All sales and marketing campaigns are to be submitted on form S-101(appendix A) to the I3 BROADBAND CEO for approval. If customers' CPNI information is to be used in the campaign, a completed and signed form O-101 (appendix B), per customer, must accompany the S-101 form upon submission. Sales and marketing campaigns WILL NOT be approved without the appropriate paperwork completed and signed. Electronic and verbal submissions WILL NOT be accepted.
2. Forms S-101's and O-101's will be submitted to and maintained by the accounting department for no less than one (1) year.

Permissible Use of CPNI in Sales

1. Sales staff may use or disclose CPNI in order to market services that are within the same category of services to which the customer presently subscribes. For example, sales staff can use or disclose CPNI information to sell additional local services to an existing local service subscriber. Sales staff may disclose CPNI without prior authorization in order to offer additional services associated with subscribed services, such as customer premise equipment, call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion. Likewise sales staff can use CPNI to market services formerly known as adjunct-to-basic services, including, but not limited to, speed-dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features. Further, if a customer is subscribed to more than one category of service offered by a carrier (i.e., both local and wireless services), a carrier is permitted to share CPNI between the different affiliated entities that provide the subscribed services, provided the customer subscribes to each service.
2. Please refer to the CPNI compliance Manual's "Use of CPNI without Customer Approval" page 4 and "Frequently Asked Questions" page 9.

Non-Permissible Use of CPNI in Sales

1. Sales staff are not permitted to disclose CPNI without prior authorization to a service provider to whom a customer is not already subscribed. Sales staff are also prohibited from using CPNI to identify or track customers that call competing service providers. For example, staff may not use CDR records to track all customers that call local service competitors.

2. Please refer to the CPNI compliance Manual's "Use of CPNI without Customer Approval" page 4.

I3 BROADBAND Company CPNI Policies

Opt-in

1. Before I3 BROADBAND will share or disclose CPNI for the purpose of marketing both communications-related and non-communications-related services with joint venture partners, independent contractors, or third parties separate from I3 BROADBAND, an "opt-in" (form O-101) approval will be obtained from each customer involved. This means that before I3 BROADBAND will disclose information to a third party, I3 BROADBAND will seek informed consent in a formally executed notification returned by the customer.
2. Completed form O-101's will be submitted to and maintained by the accounting department for no less than one (1) year.

Opt-out Mechanism Failure

1. I3 BROADBAND will provide written notice using Form O-103 (Appendix D) within five (5) business days to the FCC of any instance where opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

Unauthorized Access to CPNI

1. Should unauthorized access to a customer's CPNI be obtained, I3 BROADBAND will send an electronic notification to the United States Secret Service ("USSS") and the Federal Bureau of Investigations ("FBI") through the FCC link http://www.fcc.gov/eb/cpni. This notification will be sent within seven (7) business days after reasonable determination that a breach has occurred and will contain the following information:
    a. Dates of discovery and notification
    b. Detailed description of the CPNI that was the subject of the breach
    c. Circumstances of the breach
2. I3 BROADBAND will then notify the customer of the unauthorized access.
3. A copy of the notification (Appendix C) will be submitted to and maintained by the accounting department for no less than two (2) years.

Additional Measures to Protect CPNI Information

1. The servers that run I3 BROADBAND databases are locked down from access outside of the I3 BROADBAND network. This means that unless you are directly connected to the I3 BROADBAND network, you would be unable to gain remote administration to these servers.
2. I3 BROADBAND utilizes VPN for all devices that require remote administration. A VPN client certificate, that is specific to the VPN firewall on the I3 BROADBAND network, is required for I3 BROADBAND network technicians to gain access to anything on the I3 BROADBAND network through the Internet. Access to the I3 BROADBAND network, without a VPN client certificate, is not a possibility.
3. I3 BROADBAND has implemented real-time monitoring of our entire network core for intrusion detection and remote attacks. I3 BROADBAND has setup predefined automatic email responses to a vast number of known threats. This allows I3 BROADBAND network technicians to monitor the network 24 hours a day, 7 days a week. Ninety-nine percent of I3 BROADBAND network attacks are stopped by automatic scripted responses.

-- Appendix A --

Form S-101

Sales and Marketing Campaign Proposal

Name of Company Presenting the Campaign:

_____

Start and End Date: _____

Will this campaign require the use of CPNI information? ☐ Yes ☐ No

** Signed Form O-101's must be attached if CPNI information is to be used **

If yes, what type of CPNI will be used in the campaign?

_____

_____

_____

What products and services will be offered in this campaign?

_____

_____

_____

_____

_____

_____

Submitted By: _____ Approved By: _____

(CEO Signature)

Date: _____ Date: _____

-- Appendix B –

Form O-101

Customer Proprietary Network Information

Dear Valued Customer,

In order to continue to provide excellent products and services, I3 BROADBAND gathers information about the quality, type, destination, technical configurations, and amount of products and services you use. This information is called Customer Proprietary Network Information ("CPNI").

Please be advised that under federal regulations, you have a right, and I3 BROADBAND has a duty, to protect the confidentiality of your CPNI. I3 BROADBAND will not disclose or sell your CPNI without receiving prior authorization, or unless required to do so by operation of law. We will also discontinue using your information upon request.

To continue to serve you in the most effective and efficient manner, we would like to use your CPNI for purposes of determining the best products and services that will benefit you. By opting-in, I3 BROADBAND may also disclose, share or permit access to your CPNI on a limited, as-needed basis with trusted agents and contractors that assist us in providing you with communications-related services.

Please note that we will continue to rely upon this authorization until you have notified us of any limitations on the use of your CPNI. Also, please be aware that denial of authorization will not affect your current telecommunications service.

In order for us to begin better serving you, please check the appropriate box below and return this form to our mailing address:

I3 BROADBAND
602 Highpoint Lane
East Peoria, IL 61611

☐ I authorize I3 BROADBAND to share my CPNI information with trusted agents.

☐ I do not authorize I3 BROADBAND to share my CPNI information with trusted agents.

_____
(Signature of Authorized Person)

Date: _____

-- Appendix C --

Form O-102

Unauthorized Access Notification

I3 BROADBAND
602 High Point Lane
East Peoria, IL 61611

Date of Access: _____

Date of Discovery: _____

Date of Law Enforcement Notification: _____

Date of Customer Notification: _____

Submitted By: _____

Please give a detailed description of the CPNI that was the subject of the breach:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Please describe the circumstances of the breach:

_____

_____

_____

_____

_____

_____

-- Appendix D --

Form O-103

Opt-out Mechanism Failure Notification

I3 BROADBAND
602 High Point Lane
East Peoria, IL 61611

Date: _____

Submitted By: _____

Please give a detailed description of how the Opt-out Mechanism Failed:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____